REMARKS

Claims 1-21 are rejected in view of LIU and NEWMAN. Reconsideration of the rejection in view of the following comments is respectfully solicited.

The Examiner has indicated that the arguments filed on October 10, 2004 have been fully considered, but are not deemed to be persuasive. Applicant pointed out that the prior art verification process is cumbersome and that that the prior art key revocation process does not work well. The Examiner responds that "the features upon which applicant relies (i.e., the above points that are enumerated above) are not recited in the rejected claims". Applicant is not claiming a cumbersome prior art verification process and/or a key revocation process that does not work well. So, of course, the claims do not include these limitations.

The point of the argument was to demonstrate that the prior art, such as relied upon by the Examiner, is *different* than the claimed invention. The claims recite features that are not in the prior art. The cumbersome prior art verification process and inefficient key revocation process do not form part of the claimed invention, they should be contrasted with the claimed invention. Reconsideration of applicant's argument is respectfully requested.

The Examiner also dismissed applicant's argument that the prior art does not include the operations of "periodically sending a verification request from the server to the client asking if the client public key remains valid" and "removing or deleting key information". The Examiner maintains that NEWMAN teaches "periodically sending a verification request from the server to the client asking if the client public key remains valid". NEWMAN only teaches about populating (adding) public keys. Nothing in NEWMAN shows or suggests any type of technique for deleting public keys at a server, as claimed.

The CDC of NEWMAN periodically makes automatic checks and updates all the existing phone numbers and public keys contained *within clients (facsimile terminal units)*. (Column 6, Lines 1-5) Thus, NEWMAN updates, adds, populates *client* machines with new public keys. The Examiner also relies upon the fact that NEWMAN discloses that all new FAX units (client terminals) going on-line into the network must initially register with the CDC (Central Database Controller). This server thus has available in one of its memory units the public key registry for each new subscriber as well as the public key for each older subscriber. (Column 5, Lines 58-62)

Again, NEWMAN is teaching how to update, add or populate public keys at a server, but there is no teaching at all with respect to deleting keys from the server. In particular, nothing in NEWMAN shows or suggests the operation of "periodically sending a verification request from the server to the client asking if the client public key remains valid". Adding new keys to a client machine, which NEWMAN does perform, in no way shows or suggests "periodically sending a verification request from the server to the client asking if the client public key remains valid." NEWMAN never shows or suggests a server querying a client to determine if the client public key remains valid. NEWMAN only adds public keys to a client machine. These public keys are for other machines. Thus, these public keys have nothing to do with "querying a client to determine if the client public key remains valid."

In column 10 of NEWMAN there is a teaching regarding an unresponsive client machine. NEWMAN teaches that "If data cannot be acquired from the user site, a fixed charge of $25 will be assigned. This charge will be adjusted the next time the user turns on their computer or FAX machine since the first task of the security device will be the sending of this data to the local site. If after 15 days, no data is still received by the local site, the user site will be notified, and the security device functioning will be suspended until this data is downloaded to the local central site." Nowhere in this description of a FAX security system is there any teaching that shows or suggests the claimed method for managing public keys through a server. In particular, NEWMAN does not show or suggest the claimed operation of "periodically sending a verification request from the server to the client asking if the client public key remains valid" and "if an affirmative response to the verification request is not received, removing the client public key from the database." NEWMAN does not show or suggest any mechanism for "asking if the client public key remains valid". Furthermore, there is no teaching whatsoever in NEWMAN regarding removing a client public key from a database if an affirmative response to a verification request is not received.

The Examiner maintains that "the CDC has a capability of removing public keys that are no more in service. CDC/central server will figure out the validity of the public keys (whether or not they need updates (removing/changing to the new one's), since all the periodically after hour checks are made by the server on each of the terminals. [Column 6, lines 1-3] and at the same time each terminals or clients updates and maintains its own internal table of FaxPhone numbers and public keys. [Column 6, lines 3-5]" The Examiner's position is not based upon any actual teaching in NEWMAN. Rather, the Examiner says that "the CDC has a capability", without substantiating this with any specific teaching. Similarly, the Examiner states that the "the CDC/central server will figure out the validity of the public keys". That is the Examiner's position, nothing in NEWMAN addresses this topic. NEWMAN only teaches *adding* keys to a system. In one instance, keys are added from the server to the client machine. In the other instance, when a new client machine is added to the network, it registers with the server. NEWMAN only teaches additive operations. The Examiner's speculative positions about what the system might do, relying upon the teachings of the present invention, are inappropriate.

In sum, NEWMAN never addresses the issue of removing or deleting key information. NEWMAN only discusses adding new public keys associated with new FAX units being added to the network. Even assuming for the sake of argument that NEWMAN inherently has some type of revocation process, then NEWMAN is merely operating in accordance with a "certificate revocation list" technique. As discussed in the background of the invention, such a prior art approach is problematic. In sum, NEWMAN, at best, teaches a "certificate revocation list" technique that is known in the prior art as a flawed mechanism. The invention overcomes the problems associated with a "certificate revocation list".

LIU does not rectify the deficiencies of NEWMAN. The LIU reference discloses an "identity authority" of the type discussed in the background of the invention. In LIU, the user, not the server, initiates the removal of a key. Once a user has initiated the process of removing a key, the server generates "a confirmation request", which is sent to the user. See, e.g., column 29, lines 21-40. A "confirmation request" is confirming an action initiated by the user. This stands in sharp contrast to the claimed invention.

The independent claims include a number of limitations that are not shown or suggested by LIU. For example, claim 1 recites "periodically sending a verification request from the server to the client asking if the client public key remains valid". First, observe that the server, not the user, initiates this action. This is in contrast to LIU, where the user initiates the action. Next, observe that the server is sending a "verification request" to test the user's existence. In LIU, the user's existence is known, because the user initiated the request. The "confirmation request" in LIU is not a "verification request". The "confirmation request" in LIU operates to provide the user with a second chance to endorse the user-initiated process of removing a key. Thus, LIU does not show or suggest the claimed server initiated operation. Further, LIU does not show or suggest the use of the claimed verification request.

In sum, claim 1 includes a number of limitations that are not shown or suggested by the prior art. Thus, claim 1 should be in a condition for allowance. Claims 2-7 are dependent upon claim 1 and therefore should also be in a condition for allowance. Claim 8 includes limitations of the type discussed in connection with claim 1. Thus, claim 8 and its dependent claims 9-14 should also be in a condition for allowance. Similarly, claim 15 includes limitations of the type discussed in connection with claim 1. Thus, claim 15 and its dependent claims 16-21 should also be in a condition for allowance.

If there are any residual prosecution issues that can be resolved with a telephone call, the Patent Examiner is requested to contact the undersigned.

Dated: 5-10-05

Respectfully submitted,
COOLEY GODWARD LLP

By: ______________________
William S. Galliani
Reg. No. 33,885

Cooley Godward LLP
ATTN: Patent Group
Five Palo Alto Square
3000 El Camino Real
Palo Alto, CA 94306-2155
Tel: (650) 843-5000
Fax: (650) 857-0663